Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та управління

Кафедра інформаційної та кібернетичної безпеки

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ О.Б. Жильцов
«__» _____ 2018 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Протокол № 0942/16
(підпис) (прізвище, ініціали)
«__» _____ 2016 р.

Київ – 2018

Розробник:

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Викладач:

Аносов Андрій Олександрович, кандидат військових наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки Факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки

Протокол від 13.09.2018 р. № 6

Завідувач кафедри _____ В.Л. Бурячок
(підпис)

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 20___ р.

Керівник освітньої програми _____ (В.В. Семко)
(підпис)

Робочу програму перевірено

___.___. 20___ р.

Заступник директора/декана _____ І.Ю. Мельник
(підпис)

Пролонговано:

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	нормативна	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	5 / 150	
Курс	3	
Семестр	5	
Кількість змістових модулів з розподілом:	5	
Обсяг кредитів	5	
Обсяг годин, в тому числі:	150	
Аудиторні	70	
Модульний контроль	8	
Семестровий контроль	60	
Самостійна робота	12	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Захист інформації в інформаційно-комунікаційних системах» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека, освітньої 125.00.01 «Безпека інформаційних і комунікаційних систем».

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач другого (магістерського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Захист інформації в інформаційно-комунікаційних системах» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Захист інформації в інформаційно-комунікаційних системах» складається з п’яти змістових модулів: Методи виявлення та оцінки загроз інформації; Визначення вихідних даних щодо створення КСЗІ в ІТС; Формування моделі загроз безпеки інформації в ІТС; Формування моделі порушника безпеки інформації в ІТС; Формування політики безпеки інформації в ІТС. Обсяг дисципліни – 150 год. (5 кредитів).

Метою викладання навчальної дисципліни «Захист інформації в інформаційно-комунікаційних системах» є формування у студентів уміння вирішувати задачі аналізу середовищ функціонування програмних та програмно-апаратних комплексів в інформаційно-телекомунікаційних (автоматизованих) системах, формування політики безпеки інформації в ІТС, застосовувати нормативно-правові, організаційні та технічні процедури підготовки до впровадження комплексних систем захисту інформації.

Завдання полягає у формуванні теоретичних знань та практичних умінь у сфері інформаційної та кібернетичної безпеки та набуття **наступних компетентностей**:

Фахові компетентності
КФ-3: Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
КФ-5: Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
КФ-7: Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- процеси захисту інформаційно-телекомунікаційних (автоматизованих) систем від порушників безпеки інформації;
- методи та види несанкціонованого доступу та канали витоку інформації в інформаційно-телекомунікаційних (автоматизованих) системах;
- методику визначення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних та автоматизованих системах;
- принципи протидії несанкціонованому доступу до ресурсів і процесів в ІТС;
- функції та особливості реалізації системи захисту інформації в інформаційних, інформаційно-телекомунікаційних та автоматизованих системах.

уміти:

- аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних;
- застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектури операційних систем;
- виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної та/або кібербезпеки в ІТС;
- вирішувати задачі підготовки вихідних даних до проектування комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;
- здійснювати оцінку рівня захищеності інформації що обробляється в ІТС та оцінки наявності потенційних вразливостей.

та досягти наступних **програмних результатів навчання:**

ПРз-2: здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій; розробляти та аналізувати проекти ІТС базуючись на стандартизованих технологіях та протоколах передачі даних; застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектури операційних систем; здійснювати захист ресурсів і процесів в ІТС на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування ІТС; виконувати аналіз програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної та/або кібербезпеки в ІТС.

ПРз-3: забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих)

систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.

ПРз-7: вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах; здійснювати оцінку рівня захищеності інформації що обробляється в ІТС використовувати інструментальні засоби оцінювання наявності потенційних вразливостей; вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих); вирішувати задачі експертизи, випробування КСЗІ.

ПРз-11: забезпечувати процеси моніторингу доступу до ресурсів і процесів ІТС; забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в ІТС.

ПРз-12: виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних та автоматизованих системах; аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в ІТС; аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Методи виявлення та оцінки загроз інформації							
Тема 1. Методи виявлення та оцінки загроз інформації	16	8		6			2
Разом	16	8		6			2
Змістовий модуль 2. Визначення вихідних даних щодо створення КСЗІ в ІТС							
Тема 2. Визначення вихідних даних щодо створення КСЗІ в ІТС	16	2		2	10		2
Модульний контроль	2						
Разом	18	2		2	10		2
Змістовий модуль 3. Формування моделі загроз безпеки інформації в ІТС							
Тема 3. Формування моделі загроз безпеки інформації в ІТС	16	2		2	10		2
Модульний контроль	2						
Разом	18	2		2	10		2
Змістовий модуль 4. Формування моделі порушника безпеки інформації в ІТС							
Тема 4. Формування моделі порушника безпеки інформації в ІТС	17	2		2	10		3

Модульний контроль	2						
Разом	19	2		2	10		3
Змістовий модуль 5. Формування політики безпеки інформації в ІТС							
Тема 5. Формування політики безпеки інформації в ІТС	17	4		2	8		3
Модульний контроль	2						
Разом	19	4		2	8		3
Курсова робота	30						
Підготовка та проходження контрольних заходів	30						
Усього	150	18		14	38		12

5. Програма навчальної дисципліни

Змістовий модуль 1. Методи виявлення та оцінки загроз інформації

Основні питання:

- Методи та види несанкціонованого доступу та канали витоку інформації
- Поняття дестабілізуючих факторів та моделі реалізації загроз інформації
- Методи оцінки загроз інформації
- Структура критеріїв захищеності інформації та послуг, що забезпечують захист від загроз
- Нормативно-правові акти у сфері захисту інформації
- Основні нормативно-правові акти, що регламентують питання захисту інформації в ІКС

Змістовий модуль 2. Визначення вихідних даних щодо створення КСЗІ в ІТС

Основні питання:

- Порядок обстеження середовищ функціонування ІТС
- Обстеження середовищ функціонування ІТС підприємства
- Формування вихідних даних щодо створення КСЗІ в ІТС

Змістовий модуль 3. Формування моделі загроз безпеки інформації в ІТС

Основні питання:

- Порядок формування моделі загроз безпеки інформації в ІТС
- Порядок визначення загроз безпеки інформації підприємства
- Формування моделі загроз безпеки інформації в ІТС

Змістовий модуль 4. Формування моделі порушника безпеки інформації в ІТС

Основні питання:

- Характеристики порушників безпеки інформації. Модель порушника
- Порядок визначення порушників безпеки інформації підприємства
- Формування моделі порушника безпеки інформації в ІТС

Змістовий модуль 5. Формування політики безпеки інформації в ІТС

Основні питання:

- Поняття політика безпеки інформації
- Профіль безпеки інформації в ІТС
- Формування політики безпеки інформації в ІТС в ІТС
- Порядок формування політики безпеки інформації в ІТС в ІТС

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, залік.
- *Комп'ютерного контролю:* програми - емулятори.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Ma	Модуль 1	Модуль 2	Модуль 3	Модуль 4	Модуль 5

	максимальна кількість балів за одиницю	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	4	4	1	1	1	1	1	1	2	2
Відвідування семінарських занять	1										
Відвідування практичних занять	1	3	3	1	1	1	1	1	1	1	1
Відвідування лабораторних занять	1			5	5	5	5	5	5	4	4
Робота на семінарському занятті	10										
Робота на практичному занятті	10	3	30	1	10	1	10	1	10	1	10
Лабораторна робота (в тому числі допуск, виконання, захист)	10			5	50	5	50	5	50	4	40
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5	1	5
Виконання модульної роботи	25			1	25	1	25	1	25	1	25
Виконання ІНДЗ	30										
Разом		-	42	-	97	-	97	-	97	-	87
Максимальна кількість балів: 420											
Розрахунок коефіцієнта: 420/60=7											

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Методи виявлення та оцінки загроз інформації		2	5
1	Методи виявлення загроз інформації. Оцінка загроз інформації: • виконання завдань відповідно до теми; • опрацювання фахових видань.	2	5
Змістовий модуль 2. Визначення вихідних даних щодо створення КСЗІ в ІТС		2	5
2	Обстеження середовищ функціонування комп'ютерних мереж: • виконання завдань відповідно до теми; • опрацювання фахових видань.	2	5
Змістовий модуль 3. Формування моделі загроз безпеки інформації в ІТС		2	5
3	Визначення моделі загроз безпеки інформації в ІТС: • виконання завдань відповідно до теми; • опрацювання фахових видань.	2	5
Змістовий модуль 4.Формування моделі порушника безпеки інформації в ІТС		3	5
4	Визначення моделі порушника безпеки інформації в ІТС: • виконання завдань відповідно до теми; • опрацювання фахових видань.	3	5
Змістовий модуль 5. Формування політики безпеки інформації в ІТС		3	5
5	Визначення політики безпеки інформації в ІТС: • виконання завдань відповідно до теми; • опрацювання фахових видань.	3	5
	Разом	12	25

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – тест, що складається 3 комплексних запитань.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі заліку, умовою допуску до якого є отриманням студентом 35 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комбінована. Екзамен оцінюється у 40 балів за розподілом:

20 балів – комплексний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями з побудови інформаційних мереж та управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

Оцінювання практичного завдання відбувається в межах від 0 до 20 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь необхідних для побудови захищених інформаційних та інформаційно-телекомунікаційних (автоматизованих) систем.

Бали за виконання тесту та бали за виконання практичного завдання додаються. Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на екзамені, представлене у таблиці.

Підсумкова кількість балів (max – 40)	Оцінка за 4-бальною шкалою
1 – 23	«незадовільно»
24 – 29	«задовільно»
30 – 35	«добре»
36 – 40	«відмінно»

Орієнтовний перелік питань для семестрового контролю

1. Фактори (технологічні та науково-технічні), що впливають на необхідність захисту інформації
2. Види інформації відповідно Закону України "Про інформацію".
3. Властивості інформації.
4. Характерні особливості інформації для захищених ІТС
5. Загрози безпеці інформації та інформаційних ресурсів.
6. Джерела загроз безпеці інформації та інформаційних ресурсів.
7. Характеристика загальних принципів захисту інформації.
8. Заходи, що виконує система захисту інформації.
9. Принципи побудови типової система захисту інформації
10. Характеристика канального шифрування.
11. Характеристика абонентського шифрування.
12. Протокол міжмережного захисту Kerberos
13. Класифікація віддалених атак.
14. Середовища, в яких знаходиться інформації та групи факторів, що впливають на забезпечення інформаційної безпеки.
15. Зміст обстеження обчислювальної системи ІТС.
16. Зміст обстеження фізичного середовища.
17. Зміст обстеження середовища користувачів.
18. Зміст обстеження інформаційного середовища та технології обробки інформації
19. Зміст Моделі порушника.
20. Навмисні загрози інформації
21. Ресурси, що підлягають захисту
22. Зміст робіт із захисту інформації від несанкціонованого доступу.
23. Документи із захисту інформації від витоку її технічними каналами
24. Випадкові загрози інформації та загрози об'єктивного характеру
25. Типи загроз інформації
26. Методи оцінки можливих загроз інформації
27. Класифікація загроз інформації за впливом (характером)

28. Класифікація загроз інформації за наслідками
29. Зміст загроз конфіденційності, цілісності, доступності, спостереженості.
30. Зміст обстеження обчислювальної системи ІТС.
31. Зміст обстеження фізичного середовища.
32. Зміст обстеження середовища користувачів.
33. Зміст обстеження інформаційного середовища та технології обробки інформації
34. Зміст Моделі порушника.
35. Напрями забезпечення захисту інформації в інформаційних і комунікаційних системах
36. Найбільш поширені сценарії несанкціонованого доступу до інформації.
37. Загальні принципи захисту інформації.
38. Елементи системи інформаційної безпеки щодо захисту інформації.
39. Завдання фахівців з планування комплексних систем інформаційної безпеки.
40. Середовища виникнення джерел загроз інформації.
41. Способи несанкціонованого доступу до інформації.
42. Метод реалізації несанкціонованого доступу до інформації Обхідний шлях.
43. Метод реалізації несанкціонованого доступу до інформації Троянський кінь
44. Метод реалізації несанкціонованого доступу до інформації Логічна бомба
45. Метод реалізації несанкціонованого доступу до інформації Атака
46. Метод реалізації несанкціонованого доступу до інформації Між рядків
47. Метод реалізації несанкціонованого доступу до інформації Аналіз трафіку
48. Метод реалізації несанкціонованого доступу до інформації Розрив лінії
49. Метод реалізації несанкціонованого доступу до інформації Маскарад
50. Метод реалізації несанкціонованого доступу до інформації Підкладення свині
51. Метод реалізації несанкціонованого доступу до інформації Повторне використання ресурсів
52. Метод реалізації несанкціонованого доступу до інформації Використання комп'ютерного вірусу
53. Метод реалізації несанкціонованого доступу до інформації Використання програми-імітатора
54. Структура типової системи захисту інформації.
55. Завдання підсистеми захисту локальних робочих місць.
56. Завдання підсистем захисту локальної обчислювальної мережі та межмережевої взаємодії.
57. Завдання підсистеми контролю і реєстрації.
58. Характеристика загальних принципів захисту інформації.
59. Заходи, що виконує система захисту інформації.
60. Принципи побудови типової система захисту інформації

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов’язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов’язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або

		професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов’язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 150 год., лекції – 9 год., практичні заняття – 14 год., лабораторні роботи – 38 год., модульний контроль –8 год., самостійна робота –56 год.

Модулі (назви, бали)	**Змістовий модуль 1. Методи виявлення та оцінки загроз інформації (42 бали)**				**Змістовий модуль 2. Визначення вихідних даних щодо створення КСЗІ в ІТС (97 балів)**	
Лекції (теми, бали)	Методи та види несанкціонованого доступу та канали витоку інформації (1 бал)	Поняття дестабілізуючих факторів та моделі реалізації загроз інформації (1 бал)	Методи оцінки загроз інформації (1 бал)	Структура критеріїв захищеності інформації та послуг, що забезпечують захист від загроз (1 бал)	Порядок обстеження середовищ функціонування ІТС (1 бал)	
Практичні, семінарські заняття (теми, бали)	Нормативно-правові акти у сфері захисту інформації (22 балів)	Основні нормативно-правові акти, що регламентують питання захисту інформації в ІКС. (11 балів)				Формування вихідних даних щодо створення КСЗІ в ІТС (11 балів)
Лабораторні заняття (теми, бали)					Обстеження середовищ функціонування ІТС підприємства (55 балів)	
Самостійна робота	Самостійна робота (5 балів)				Самостійна робота (5 балів)	
Поточний контроль (вид, бали)					Модульна контрольна робота 1 (25 балів)	

Модулі (назви, бали)	**Змістовий модуль 3. Формування моделі загроз безпеки інформації в ІТС (97 балів)**		**Змістовий модуль 4. Формування моделі порушника безпеки інформації в ІТС (97 балів)**		**Змістовий модуль 5. Формування політики безпеки інформації в ІТС (87 балів)**	
Лекції (теми, бали)	Порядок формування моделі загроз безпеки інформації в ІТС. (1 бал)		Характеристики порушників безпеки інформації. Модель порушника (1 бал)		Поняття політика безпеки інформації (1 бал)	Профіль безпеки інформації в ІТС (1 бал)
Практичні, семінарські заняття (теми, бали)		Формування моделі загроз безпеки інформації в ІТС. (11 балів)		Формування моделі порушника безпеки інформації в ІТС. (11 балів)		Формування політики безпеки інформації в ІТС в ІТС (11 балів)
Лабораторні заняття (теми, бали)	Порядок визначення загроз безпеки інформації підприємства (55 балів)		Порядок визначення порушників безпеки інформації підприємства (55 балів)		Порядок формування політики безпеки інформації в ІТС (44 бали)	
Самостійна робота	Самостійна робота (5 балів)		Самостійна робота (5 балів)		Самостійна робота (5 балів)	
Поточний контроль (вид, бали)	Модульна контрольна робота 2 (25 балів)		Модульна контрольна робота 3 (25 балів)		Модульна контрольна робота 4 (25 балів)	
Підсумковий контроль (вид, бали)	Екзамен (40 балів)					

8. Рекомендовані джерела

Основна (базова):

1. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.
2. Бурячок В. Л.Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.
3. Бурячок В. Л.Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с
4. Олейник А.И. Методологические основы управления ИТ-инфраструктурой предприятия. Раздел в кн.: Техника и технология в XXI веке: современное состояние и перспективы развития: монография/ И.П. Болодурина, А.С. Дулесов, Р.А. Загидуллин, А.В. Зарипов, Н.Ф. Локтев, Ю.П. Луговскова, С.В. Лукашенко, Н.И. Москаленко, Л. Найзабаева, А.И. Олейник, В.И. Рассоха, М.С. Садыкова, Я.С. Сафиуллина, Е.Н. Ткачева, С.С. Чернов , 2009. С. 228—245.
5. Комп'ютерні мережі: навч. посіб. для технічних спец. вищих навч. закл. Кн. 2. - Львів: Магнолія 2006, 2014. - 327 с.
6. Богуш В.М., Юдін О.К. Основи інформаційної безпеки держави. – К.: "МК-Прес", 2005 – 432 с.
7. Богуш В.М., Кудін А.М. Інформаційна безпека від А до Я: 3000 термінів і понять. - К.: МОУ, 1999. - 456 с.
8. ДСТУ 2462--94. Сертифікація. Основні поняття. Терміни та визначення.- К.: Держстандарт України, 1994. - 24 с.
9. ДСТУ 2874--94. Системи обробки інформації. Бази даних. Терміни та визначення.
10. ДСТУ 2938--94. Системи оброблення інформації. Основні поняття. Терміни та визначення.
11. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

Додаткова

1. Руководство по технологиям объединенных сетей. 3-е издание. Пер. с англ. М.: Издательский дом «Вильямс», 2002.
2. Вегешна Шринивас. Качество обслуживания в сетях IP. Пер. с англ. М.: Издательский дом «Вильямс», 2003.
3. Scott Mueller. Upgrading and Repairing Networks, Third Edition. Que, 2002.
4. Panoc C. Lekkas. Network Processors. The McGraw-Hill Companies, 2003.
5. International Standard ISO/IEC 17799. Information technology - Code of practice for information security management. First edition 2000-12-01.
6. International Standard ISO 7498-2: 1989 Information processing systems. - Open Systems Interconnection. - Basic Reference Model. - Part 2: Security Architecture. - First edition. -15.02.1989. - 32 p.ДСТУ 2226--93. Автоматизовані системи. Терміни та визначення.
7. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000 С.26-120
8. Уфимцев Ю.С. Методика информационной безопасности / Уфимцев Ю.С., Буянов В.П., Ерофеев Е.А. и др. – М.: Издательство "Экзамен", 2004. – 544с.

9. Додаткові ресурси

1. Руководства пользователя коммутаторов D-Link и учебные материалы компании D-Link [электронный ресурс] ftp://ftp.dlink.ru/

2. Бараш Л. Коммутаторы в локальных сетях. [электронный ресурс] http://desna.kiev.ua

3. History of LAN Switching. [электронный ресурс] http://www.myipaddressinfo.com

4. Evolution: 20 years of switching fabric. Ori Aruj, Dune Networks [электронный ресурс] http://www.commsdesign.com

5. On-chip Global Interconnects for Networking ASICs [электронный ресурс] http://www.lsi.com

6. Andreas D. Bovopoulos and Micha Zeiger. Shared-Memory Fabrics Meet 10-Gbit Backplane Demands. TeraChip, Inc. [электронный ресурс] http://www.commsdesign.com

7. Matching Output Queueing with a Combined Input Output Queued Switch [электронный ресурс] http://www-rcf.usc.edu

8. An improved algorithm for CIOQ switches. Yossi Azar, Ybssi Richter. [электронный ресурс] http://portal.acm.org

9. Сайт научной базы данных «SciVerse ScienceDirect» [электронный ре-сурс] http://www.sciencedirect.com

10. Сайт Института инженеров по электротехнике и электронике (IEEE,

11. Institute of Electrical and Electronics Engineers) [электронный ресурс] http://www.ieee.org